REMARKS/ARGUMENTS

This paper is being provided in response to the Final Office Action dated July 24, 2007 for the above-referenced application. In this response, Applicant has added new Claims 66-71. Applicant respectfully submits that the newly added claims are supported by the originally filed application.

The rejection of Claims 1-7, 22-28 and 41-52 and 63-65 under 35 U.S.C. § 103(a) as being unpatentable over Waldin et al (U.S. Patent No. 6,094,731 hereinafter referred to as "Waldin") in view of Drew (U.S. Patent No. 6,928,555, hereinafter "Drew") is hereby traversed and reconsideration thereof is respectfully requested.

Claim 1 recites a computer implemented method of scanning a storage device for viruses, comprising: determining physical portions of the storage device that have been modified since a previous virus scan using information about the physical portions without using information about a file structure, a file system, or a file type; detecting, by the storage device, write operations to tracks of the storage device; providing, to an antivirus unit by the storage device, information indicating which tracks of the storage device have been accessed for a write operation; and scanning, by the antivirus unit, at least parts of the physical portions for viruses, wherein scanning is performed without using information about a file structure, a file system, or a file type, and wherein scanning is performed on those tracks to which write operations have been directed in accordance with the information provided by the storage device. Claims 2-4, and 63 depend from Claim 1.

Claim 22 recites a computer program product for scanning a storage device for viruses, the computer program product including a computer-readable medium with executable code stored thereon for: determining physical portions of the storage device that have been modified since a previous virus scan using information about the physical portions without using information about a file structure, a file system, or a file type; detecting, by the storage device, write operations to tracks of the storage device; providing, to an antivirus unit by the storage device, information indicating which tracks of the storage device have been accessed for a write operation; and scanning, by the antivirus unit, at least parts of the physical portions for viruses, wherein the scanning is performed without using information about a file structure, a file system, or a file type, and wherein scanning is performed on those tracks to which write operations have been directed in accordance with the information provided by the storage device. Claims 23-25, and 64 depend from Claim 22.

Claim 41 recites an antivirus unit, comprising: means for coupling to at least one storage device; means for determining physical portions of the storage device that have been modified since a previous virus scan using information about the physical portions without using information about a file structure, a file system, or a file type; means for receiving, from the at least one storage device, information determined by the at least one storage device indicating which tracks of the at least one storage device have been accessed for a write operation; and means for scanning at least parts of the physical portions for viruses, wherein scanning is performed without using information about a file structure, a file system, or a file type, and wherein scanning is performed on those tracks to which write operations have been directed in accordance with the information provided by the storage device. Claims 42-44, 46-52, and 65 depend from Claim 41.

Waldin discloses a system, method and computer readable medium for examining a file associated with an originating computer to determine whether a virus is present within the file. (See Abstract). Waldin discloses scanning a file and placing file the identification number of each sector that is scanned into a critical sectors. As each sector is operated upon, a hash value is calculated for that sector and inserted into the critical sectors file along with the size of the file scanned. (Col. 4, Lines 52-64; Figures 1 and 2). Waldin's Figure 1 includes antivirus modules on an originating computer 2 and a recipient computer 11 and processing performed on each of the computer systems when transmitting a file from an originating computer to a recipient computer. (See Figure 1; Col. 3, Lines 22-34). Waldin's Figure 3 determines if computed hash values for file 1 match stored hash values for file 1. If not, the entire file 1 is rescanned. (Steps 36, 37 of Figure 3; Col. 6, Lines 43-46; See also Col. 2, Lines 24-26). Waldin discloses determining hash values for only those sectors of a file actually retrieved by module 5 of Figure 1. Module 3 of Waldin's Figure 1 always scans the same set of sectors of a file unless the file changes in length or the contents of those sectors changes in some way. The antivirus accelerator module 5 automatically hashes all sectors scanned by module 3 in the same way regardless of contents of the sectors. No new parser of hasher coding needs to be performed and incorporated into module 5 to support new file formats. (Col. 7, Line 35-Col. 8, Line 2).

Drew is cited on page 3 of the Office Action as support for disclosing detecting, by a storage device, write operations to tracks of the storage device; providing to an antivirus unit by the storage device information indicating which tracks of the storage device have been accessed for a write operation; and scanning portions on those tracks to which write operations have been directed in accordance with information provided by the storage device (Col. 3, Lines 40-55; Col. 4, Lines 5-25). The foregoing citations of Drew are discussed below in more detail.

Claim 1 is neither disclosed nor suggested by the references, separately or in combination, in that the references do not disclose or suggest at least the features of ***a computer implemented method of scanning a storage device for viruses, comprising: ... detecting, by the storage device, write operations to tracks of the storage device; providing, to an antivirus unit by the storage device, information indicating which tracks of the storage device have been accessed for a write operation; and scanning, by the antivirus unit, at least parts of the physical portions for viruses, ... wherein scanning is performed on those tracks to which write operations have been directed in accordance with the information provided by the storage device,*** as set forth in Claim 1.

Page 3 of the Office Action states that Waldin is silent on detecting, by the storage device, write operations to tracks of the storage device, and providing, to an antivirus unit by the storage device, information indicating which tracks of the storage device have been accessed for a write operation and scanning those tracks. Page 3 of the Office Action relies on Col. 3, Lines 40-55 and Col. 4, Lines 5-25 of Drew for disclosure of the foregoing. Col. 3, Lines 40-55 of Drew refer to steps of the flowchart of Drew's Figure 2 with respect to processing performed with reference to Figure 1 in which an antivirus program is included in the network server computer 4. After opening a file for write access (step 22), the file is scanned for viruses (step 24). If no viruses are detected, the file is provided to the application program (step 26). A period of time after the file is opened, a file closure request is made (step 28). Upon the file closure request being made, the typical antivirus program loaded into a computer system, such as network server computer 4, interfaces with the network operating system to scan the file for viruses. Col. 4, Lines 5-25 of Drew make reference to Drew's Figure 3 which includes the steps of Figure 2 with new steps 40 and 42. Step 40 determines whether a file was actually written, that is modified by the user performing some writing step on the open file. This latter citation of Drew discloses use of a modification flag set by the operating system. The computer coding for step 40 determines whether an open file was actually written or modified by looking for a flag in the operating system indicative of such a modification. Applicant's Claim 1 explicitly recites language directed to tracks of a storage device. In distinct contrast, Drew appears silent regarding any mention of a "track" of a storage device. Drew also appears silent regarding any teaching, disclosure or suggestion of the storage device detecting write operations to tracks of the storage device, and providing any information regarding the tracks from the storage device to the antivirus unit as in Applicant's Claim 1. In distinct contrast to Claim 1, Drew discloses use of a modification flag set by the operating system of the server computer 4. As pointed out above, Drew discloses that a determination as to whether a file is written or modified can be determined by the operating system when the user performs a writing step on the open file, such as when an application program issues a write operation to a file without receiving any information from the data storage device. If an operating system does not provide the modification flag, Col. 4, Lines 25-29 of Drew disclose using cache buffers to determine a "dirty cache buffer" state of the file (See, for example, Drew at Col. 4, Lines 30-50) in which cache buffers 20 are included in the server memory (See, for example, Figure 1). As such, Drew discloses the server computer 4 (not a storage device) detecting when a file (not which tracks) has been modified using information of the server computer. Furthermore, Drew makes no teaching, disclosure or suggestion of the server computer receiving any information from a storage device regarding tracks accessed for write operations. Rather, Drew's disclosure indicates that the server computer does not receive information regarding modifications from a storage device since the modification flag is set by the operating system. Thus, there appears to be no reason for the storage device to provide any information regarding write operations to the antivirus program on the computer 4 since such information is already available on the server 4 where the antivirus program resides. For at least these reasons, the references do not teach, disclose, or fairly suggest the foregoing recited features of Claim 1.

In view of the foregoing, Applicant respectfully submits that the references do not disclose or fairly suggest at least the foregoing recited features of Claim 1.

Applicant's independent Claims 22 and 41 recite features similar to those set forth above regarding Claim 1 that are neither disclosed nor suggested by the references. Thus, for reasons similar to those set forth regarding Claim 1, Applicant's Claims 22 and 41 are also neither disclosed nor suggested by the references.

Claims that depend from each of the independent Claims 1, 21, and 41 are not disclosed or suggested by the references for at least those reasons set forth above in connection with the independent claims. However, features set forth in the dependent claims are also neither disclosed nor suggested by the references.

In connection with Applicant's dependent Claim 52, page 4 of the Office Action cites to Col. 3, Lines 47-55 of Waldin as support for disclosing the recited features. Dependent Claim 52 recites, in part, ***wherein at least a portion of the antivirus unit is provided on at least some controllers for the at least one storage device***. Col. 3, Lines 47-55 of Waldin refer to Figure 1 including an originating computer 2 including modules 3, 5 and 12. Waldin discloses that file 1 included in RAM 10 could have originally been on a hard disk, floppy disk or any other computer readable medium, and could be brought into RAM 10 before being acted upon by modules 3, 5, and 12. Nowhere in this citation, or elsewhere Waldin, is there any disclosure or suggestion of including any portion of modules 3, 5, and 12 on a controller or other component of a storage device. Waldin's Figure 1 shows these modules as being included in the originating computer 2. Applicant respectfully submits that Drew also appears silent regarding any disclosure or suggestion of the features recited in Claim 52. As such, the references neither disclose nor suggest the features recited in dependent Claim 52.

In view of the foregoing, Applicant respectfully requests that the rejection be reconsidered and withdrawn.

Applicant respectfully submits that the newly added Claims 66-71 are also patentable over the cited references.

Based on the above, Applicant respectfully requests that the Examiner reconsider and withdraw all outstanding rejections and objections. Favorable consideration and allowance are earnestly solicited. Should there be any questions after reviewing this paper, the Examiner is invited to contact the undersigned at 508-898-8604.

Respectfully submitted,
MUIRHEAD AND SATURNELLI, LLC

Anne E. Saturnelli
Registration No. 41,290

MUIRHEAD AND SATURNELLI, LLC
200 Friberg Parkway, Suite 1001
Westborough, MA 01581
Tel: (508) 898-8604
Fax: (508) 898-8602

Date October 19, 2007